June 24, 2010

Senator Joseph I. Lieberman, Chairman
Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

Senator Susan M. Collins Ranking Member
Committee on Homeland Security and Governmental Affairs
350 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senators Lieberman and Collins:

Securing our nation's information infrastructure is not only important to the millions of users and businesses who depend on it for commerce, information and entertainment; it's also a matter of vital national security. Like our government, the innovative companies who develop and deploy the information technology that comprise the Internet and private networks that are part of this critical infrastructure take this very seriously. Preventing malicious attacks and protecting the data on these networks requires constant vigilance and is demanded by our customers who manage the global financial system, the power grid, communications networks, healthcare systems, and our national defense.

S. 3480, the Lieberman-Collins-Carper *Protecting Cyberspace as a National Asset Act*, is intended to protect Federal systems and critical infrastructure from cyber attack. As such, it gives new resources and power to the Department of Homeland Security over government procurement and seeks to create a new regulatory, monitoring, response, and remediation role for the DHS for both government networks *and* private, commercial networks. While well intentioned, it ultimately puts U.S. critical infrastructure at increased risk by threatening the intellectual property of American companies that create the IT that operates the vast majority of U.S. government and private-sector critical networks and systems. The unintended result may be a weakening of the domestic software and hardware industry to an extent that could, ironically, leave the U.S. *more* dependent upon foreign suppliers for their critical IT systems.

Section 253. Specifically, Section 253 mandates that the Secretary of Homeland Security (in consultation with "the Director of Cyberspace Policy, The Secretary of Commerce, the Secretary of State, the Director of National Intelligence, the Administrator of General Services, the Administrator for Federal Procurement Policy, agency CIO's, agency Chief Acquisition officers, Chief Financial Officers and the private sector") develop and implement a "supply chain risk management strategy" to protect Federal information infrastructure. This "strategy" would then be applied to the governments procurement system and in effect, regulate the information technology sector.

- All software and hardware companies who do business with the government, essentially the majority of the technology industry, would have to change their development processes, internal procedures, designs and products to comply with the "strategy." This

directly contradicts the President's proclamation in May 2009 as part of his cybersecurity strategy: "So let me be very clear. My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

- All products purchased by the government would also have to meet standards approved by NIST – hampering the ability of the government to gain access to new technology that hasn't yet been vetted by government regulators.

- This would set the barrier to entry for the government market at a prohibitive level for small businesses that would have to meet new requirements to adhere to the new regulations.

- Although the bill appears to exempt the DoD and national security systems from its requirements, as a practical matter it does not because technology products are developed through a single development process and sold globally.

- The new unbounded, government-wide procurement and testing requirements instituted by DHS would undermine international standards, including the accepted U.S. and international standard, the output-based Common Criteria ("CC"), which is intended to provide product assurance globally, prevent the balkanization of technology, and prevent foreign governments from demanding access to sensitive, proprietary technical information. The CC is already used to certify products for use in U.S. national security systems, and creating a whole new process – as Sec 253 seems likely to do – both undermines the CC, and sends a signal to other governments that non-standard, unbounded demands are acceptable. Access to this information by foreign governments could be used to create domestic competitors to U.S. firms or create other non-trivial security issues.

A better approach would be to require technology companies that do business with the Federal government to adhere to the Common Criteria where appropriate for product assurance (ensuring the product itself exhibits security), and with regard to any specific unit of production, adhere to an internationally accepted standard for 'chain-of-custody' supply chain requirements which are disclosed by the vendor, and audited pursuant to international standards. Additionally, Common Criteria should be reviewed and improved upon, so as to improve its weaknesses without losing its strengths. These programs would embrace current and insipient international standards for supply chain and software assurance. This would preserve innovation and diversity in the marketplace protecting core intellectual property. Lastly, the expertise in this area does not currently reside in the DHS, the agency granted regulatory authority under the bill.

It's also not clear whether giving significant new regulatory authority to the Department of Homeland Security is the right approach. In December the President appointed a new White House Cybersecurity Coordinator, Howard Schmidt. The Lieberman-Collins-Carper legislation appears to circumvent the Cybersecurity Coordinator's authority before the office has been given an opportunity to succeed.

Section 242. Another troubling provision in the bill as introduced is Section 242, which creates a "National Center for Cyber security and Communications" operated within DHS which would be required to "assist in the identification, remediation, and mitigation of vulnerabilities to the Federal information infrastructure *and the national information infrastructure*" including "dynamic, comprehensive, and continuous situational awareness of the security status of the national information infrastructure." There is no existing authority for the Federal government to have "continuous situational awareness" of the security status of private networks and this would be impossible to achieve without the deployment of government monitoring devices on private networks, which would also provide access to private personal and commercial data on those networks. Establishing this capability contravenes a commitment made by President Obama in his announcement of the appointment of a new White House Cybersecurity Coordinator: "Our pursuit of cybersecurity will not – I repeat, will not include – monitoring private sector networks or Internet traffic."

Section 248(b). Finally, under Section 248(b), the new DHS Cyber Director is mandated to issue regulations putting under Federal control the IT and network infrastructure of any private sector company or entity the Secretary deems important enough to be a "covered critical infrastructure" entity. This authority extends to any U.S. company determined by the Secretary to be critical, and the regulatory power is apparently unbounded.

We appreciate your attention to these important concerns and look forward to working with you to develop a more robust and secure information infrastructure.

Sincerely,

Cisco Systems, Inc.
IBM
Oracle Corporation